A Systems Approach to Homeland Security

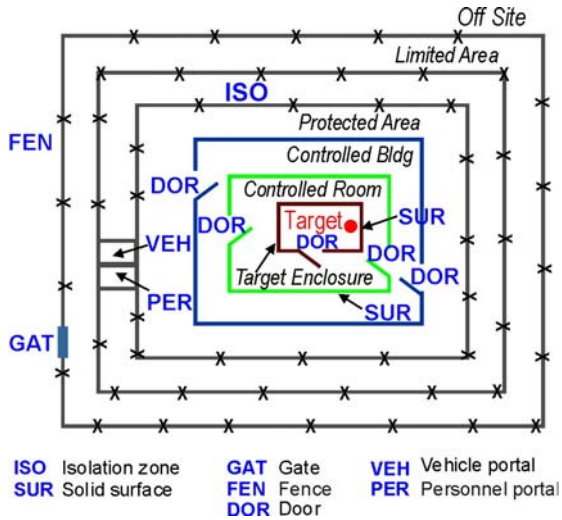
Sandia's systems approach to homeland security examines potential attacks on high-value US assets using a three-part timeline: pre-event, event, and post-event activities. The objectives are to prevent attacks from occurring, protect the asset during an attack, and respond to and recover from attacks. Analysts must:

- Understand the threat to the facility (pre-event)
- Address the vulnerabilities of the facility (event)
- Deal with the consequences of an attack on the facility (post-event)

Understanding the Threat (Pre-Event)

To reduce the likelihood of a successful attack on a US asset, analysts must understand the possible types of threats. A vigorous intelligence program gathers information from a variety of sources and works cooperatively with US agencies to anticipate where and how terrorists may strike in an effort to interdict attacks. Analysts define the attributes and characteristics of potential adversaries.

Explosives Detection



Adversary Sequence Diagram Example

An important step in preventing a catastrophic attack is to keep weapons of mass destruction out of the United States. Proactive programs with the Former Soviet Union (FSU) focus on preventing terrorists from stealing nuclear materials, while monitoring borders and checkpoints prevents these materials from leaving the FSU. Enhancing security at chemical and biological facilities and detecting explosives before they can be used help prevent attacks.

Addressing the Vulnerabilities (Event)

Analysts study the layout, security, and operations at US assets, examining a potential target in terms of possible threats. The analysts identify the most likely forms of attack and assess the vulnerabilities of the asset's protection system. Finally, they suggest ways to strengthen the protection system.

Analysts can evaluate a protection system's effectiveness *qualitatively* or *quantitatively*. In the *qualitative* approach, a team of experts surveys the facility for avenues of attack. This process can vary from simple walk-throughs to well planned and executed Red Team exercises. The advantages of the qualitative approach are that it is quick and inexpensive; the disadvantages are that subtle weaknesses can be missed and no systematic foundation is built for establishing priorities.

The *quantitative* approach uses systems analysis to develop an architecture (generally using fault trees) for the target facility that serves as the basis for the analysis. Analysts plot the potential paths an adversary could follow to achieve his goals (generally using an adversary sequence diagram). Data provided by the facility allow analysts to determine the effectiveness of the physical protection system. The results of this analysis are presented in a risk management context.

The advantages of the quantitative approach are a thorough evaluation and a prioritized list of vulnerabilities; the disadvantages include the additional time and cost required for a complete analysis. The protection system should be designed to provide layers of balanced protection-in-depth, using appropriate technologies and procedures that are properly integrated into a system that has minimal operational impact and that meets safety constraints. A well designed protection system uses elements of detection, delay, and response to defeat the adversary.

Intrusion Detection

Dealing with the Consequences (Post-Event)

If the unthinkable does occur, the nation needs to manage the consequences. When anticipating a threat that is very unlikely or very costly to address, providing consequence mitigation is a practical approach that provides contingency planning if a successful attack does occur. This activity focuses on actions that will reduce the consequences of an attack, such as planned evacuations, emergency response, crisis management, and clean-up and recovery.

Sandia Decontamination Foam

Contact:
Ron Moya
Director, Security Systems & Technology
(505) 844-3163, email: rwmoya@sandia.gov

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

5000-03-00027 2.24.03

SAND2003-3280P